Mining Rule Semantics to Understand Privacy Legislation

Travis D. Breaux and Annie I. Antón

North Carolina State University
{tdbreaux, aianton}@eos.ncsu.edu

WPES 2005, November 7th 2005

Presentation Outline

- Research Motivation
- Semantic Parameterization
- Example Semantic Models
- Parameterized Operators
- Future Work & Summary

Towards Machine-enforceable Policies

- Motivations
  - Privacy laws require companies to enforce their policies.
  - Consumers are increasingly concerned about privacy violations.
  - Companies are increasingly being held accountable for their privacy practices.

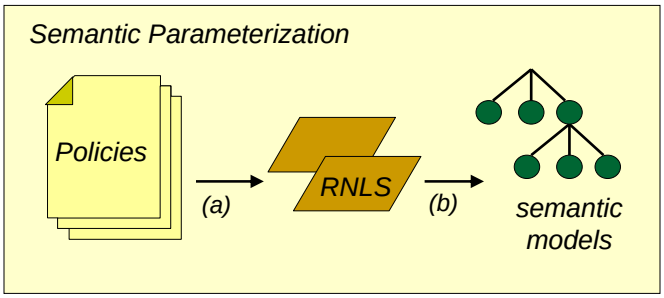
- Problem Statement

… without machine-readable and machine-enforceable policies, privacy practices will continue to be inconsistently applied and therefore prone to violations.

Need a policy language that can…

- Represent rights and obligations.
  - Rights, like permissions, describe what people and systems are ***permitted*** to do.
  - Obligations describe what people and systems are ***required*** to do.
- Interface to natural language, policies must…
  - be maintainable by non-technical policy analysts.
  - be implementable by system administrators.
  - be legally enforceable by a court of law.
- Interface to program execution, policies must…
  - exclusively decide policy-governed control flow.
  - associate governance semantics with data.

From Policies to Semantic Models



(a) Policies as Restricted Natural Language Statements (RNLS).

(b) RNLS are parameterized to build semantic models.

Simple Semantic Model
[POLICY'05]

- ***RNLS***: The provider may share information with whom?.

σ(*activity*)
α(*activity*, *actor*)
α(*activity*, *action*)
α(*activity*, *object*)
α(*activity*, *target*)

δ(*actor*, *provider*)
δ(*action*, *share*)
δ(*object*, *information*)
δ(*target*, *?whom*)

- The modal "may" indicates a *right*.

α(*provider*, *right*) δ(*right*, *activity*)

KTL Expression:

```
activity [ right : provider ] {
      actor   = provider
      action  = share
      object  = information
      target  = ?whom
}
```

Targeted and Open-ended Queries
[RE'05]

- Two types of queries:
  - Boolean queries - pair-wise relational match.
  - *Wh*-queries - pair-wise relational match with variables store corresponding values as query responses.
- Example:
  - ***What*** information may be shared with ***whom***?

ID	***Object***	***Target***
155	transaction information	subsidiary
156	experience information	affiliate
954	statistics	third-party

Example from HIPAA Privacy Rule

- Providers ***will*** <provide the patient access to their medical records> ***within*** <30 days ***of*** the patient's request>.
- Semantic models for two activities as events:
  - M_1: Patient requests access (via right).
  - M_2: Provider provides access (via obligation).
- Unit of time: 30 days.

Rule: if { M_1 } then { $M_2 <_{time}$ { 30 days $+_{time}$ M_1 } }

Arithmetic, Comparative Operators
[HIPAA Privacy Rule]

Keyword	A	C	N	HIPAA Privacy Rule Examples
less	5	1	0	Not ***less*** than 30 days before…
more	27	10	0	Contains ***more*** than 20,000 people…
before	1	9	9	At least 15 days ***before*** the…
after	20	8	2	180 days ***after*** the effective date…
older	0	1	0	Age 90 or ***older***…
smaller	0	1	0	Geographic subdivisions ***smaller*** than a state…
longer	2	7	0	No ***longer*** than 30 days from the date…

Arithmetic (A), Comparative (C), Neither (N)

Parameterized Operators

Make it possible to …

- Compare semantic models using nested properties.
  - Evaluate $E_1 < E_2$, comparing times of two events.
  - Evaluate $E_1 < T_1$, comparing an event and a time.
  - Evaluate $E_1 + T_2$, sum of time of an event and time.
- Statically detect ambiguous references.
  - Suppose E_1 has a *start* and *end* time, then which time is used to evaluate $E_1 < E_2$?

Current and Future Work

- **Case Study:** *The HIPAA Privacy Rule*, enforced by the Dept. of Health and Human Services.
  - Extracting access control rules governing use and disclosure of protected health information.
  - Representing our constraints in RBAC, XACML, Ponder.
- **Case Study:** Organizational Security Policies
  - New theory relating security requirements to business processes.
  - Framework for tracing security goals from managers to implementations by administrators.

Feedback and Questions?

To see more of our work, visit our website:

http://ThePrivacyPlace.org